Audit Report

OFFICE OF THE INSPECTOR GENERAL

QUICK-REACTION REPORT ON PHYSICAL AND SYSTEM SECURITY AT THE EAST SERVICE CENTER OF THE DEFENSE COMMISSARY AGENCY

Report Number 93-028

November 30, 1992

Department of Defense

The following acronyms are used in this report.

AIS	Automated Information System
DeCA	Defense Commissary Agency
OMB	Office of Management and Budget
SAVES	Standard Automated Voucher Examination System

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

November 30, 1992

REPORT
NO. 93-028

MEMORANDUM FOR DIRECTOR, DEFENSE COMMISSARY AGENCY

SUBJECT: Quick-Reaction Report on Physical and System Security at the East Service Center of the Defense Commissary Agency (Project No. 2AL-0035.02)

Introduction

During our audit of "Information Resources Management in the Defense Commissary Agency" (Project No. 2AL-0035), we noted that the East Service Center of the Defense Commissary Agency (DeCA) had not established procedures to satisfy the minimum security requirements prescribed by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, and the safeguards for unclassified information recommended in Office of Management and Budget Circular Number A-130, "Management of Federal Information Resources," December 12, 1985. Specifically, the East Service Center had not established procedures for accountability of users; password protection; security training and awareness; and physical control of hardware, software, and data. This matter needs your immediate action to ensure that DeCA achieves the requisite level of security to safeguard the AIS against unauthorized access and disclosure, modification, or destruction of data.

Background

On October 1, 1991, the Army, Navy, Air Force, and Marine Corps commissaries were consolidated under DeCA. DoD Directive 5105.55, "Defense Commissary Agency (DECA)," November 9, 1990, established DeCA and delegated authority to the Director of DeCA to enact the necessary security regulations for the protection of property and places. Attachment 8-3 of the "Defense Commissary Agency Missions and Functions Manual," March 1, 1991, identified the Information Resource Management Program Management Division as the Automation Security Manager for DeCA. DeCA Operations Handbook 60-1 for Fiscal Years 1991 and 1992 provided that each Region and Service Center in DeCA will have an Information Security Manager who is responsible for compliance with DeCA's Information Security Program.

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, provides mandatory minimum AIS security requirements. The Directive states that:

> Unclassified information while in AISs shall be safeguarded against tampering, loss, and destruction and shall be available when needed. This is necessary to protect the DoD investment in obtaining and using information and to prevent fraud, waste, and abuse.

The Directive further states that:

> The safeguarding of information and AIS resources . . . shall be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications, emanations security, and computer security (i.e., hardware, firmware, and software), as required.

Discussion

In evaluating security controls in DeCA, we concentrated our evaluation primarily on operations at the East Service Center. We did not review the operations at the West Service Center because it was primarily an information receiving station, and their Standard Automated Voucher Examination System (SAVES) transactions were processed at the East Service Center. Further, we did not review security procedures in regional offices because they have only query capability of the SAVES.

DeCA's East Service Center had not developed any written policies or procedures on security and had not established a formal security program for its AIS. The East Service Center's security personnel were unaware of the applicable DoD regulations, directives, or manuals concerning physical and system security. They were awaiting guidance and assistance from DeCA's security office on how to establish the procedures necessary to meet the minimum security requirements prescribed by DoD Directive 5200.28. The minimum security requirements included provisions for accountability of users; password protection; security training and awareness; and physical control of hardware, software, and data.

Accountability of users. DoD Directive 5000.28 requires that safeguards be in place to ensure that persons having access to the system can be held accountable for their actions on the system. The audit trail should, as a minimum, document the identity of each person and device having access, the time of access, and the activities that users performed, including activities that modify, bypass, or negate safeguards of the system. The SAVES at DeCA's East Service Center did not provide an "audit trail" to determine what the user did while on the system. The system also did not maintain a log of users who entered and exited the system and did not identify what transactions the users performed while in the system.

Password protection. DoD Directive 5000.28 further provides that each user has access to all information to which the user is entitled but to no more. During our audit, we noted an internal control weakness in the generation and maintenance of passwords. The East Service Center's system administrator for SAVES generated the SAVES passwords for all East and West Service Center personnel. After assigning the password to the user, he maintained a notebook record of that user's password, as well as other passwords issued. As a result, the system administrator knew the password of every person who had access to SAVES and could have used the passwords to perform the types of transactions available under those passwords. Also, if someone else obtained access to the notebook containing all passwords, that person would have the ability to obtain, modify, or possibly destroy sensitive data. We believe that it is inappropriate and unnecessary for anyone to have another user's password because the concept of password protection and accountability of the user is undermined. This could be avoided either by allowing the users to create their own passwords or by having the computer generate passwords directly to the users.

In addition, the system administrator and his alternate were designated as "super users," meaning that they could perform any function (query, insert, update, and delete data) in the SAVES system. The Chief, Information Resources Management at the East Service Center, informed us that the system administrator and his alternate needed "super user" status to create new users and to maintain the data base. As we stated in the previous paragraph, we do not believe the system administrator has the "need to know" other users' passwords. We also do not believe that the system administrator needs or should have the capability to change SAVES transaction data since DeCA had contracted out the software maintenance function for SAVES, including data base management.

Security training and awareness. DoD Directive 5200.28 provides, as a minimum security requirement, that a security training and awareness program be in place. The requirement calls for training all persons accessing the automated information system. The program should ensure that these persons are aware of proper operational and security-related procedures and risks. DeCA did not provide employees training on security-related matters, such as password and cipher lock combination protection. Also, security entrance/exit briefings were not held for employees when they received and discontinued their access to the system.

Physical control of hardware, software, and data. Initial discussions with the Chief, Information Resources Management, East Service Center, indicated that DeCA was not controlling access to its computer room because the East Service Center's security personnel were unacquainted with the DoD regulations governing physical and system security for automated data processing systems. As a result, the security personnel were unable to determine whether contractor personnel should be allowed free access with the cipher lock combination, free access without the cipher lock combination, escorted at all times, or allowed entry at all. Subsequent discussions indicate that improvements have been made and that some contractor personnel have been denied free access and the cipher code combination to the computer room. However, these denials have been made on a judgmental basis rather than being based on DeCA policy.

OMB Circular Number A-130 states that "Agencies shall maintain disaster recovery and continuity of operations plans for all information technology installations." However, the East Service Center had no contingency plan for alternate site processing for the SAVES if an event occurred that prevented normal operations or caused downtime at DeCA. As a result, operations at DeCA would cease in the event of a disaster.

Conclusion

The East Service Center had not established the minimum security requirements for its AIS because it lacked the necessary criteria as prescribed under DoD Directive 5200.28 and Office of Management and Budget Circular Number A-130. Procedures had not been implemented for accountability of users; password protection; security training and awareness; and physical control of hardware, software, and data. The Defense Commissary Agency should take immediate actions to comply with the minimum security requirements of DoD and Office of Management and Budget's established guidance.

Recommendations for Corrective Action

We recommend that the Director, Defense Commissary Agency, direct the East Service Center to implement a formal security program with written policies and procedures on physical and system security, in accordance with DoD Directive 5200.28. As a minimum, the program should:

1. Limit the System Administrator's access to the data base, so that this person would not have the capability to execute transactions.

2. Implement procedures whereby the password is either developed by the user or randomly generated by the computer directly to the user to protect the confidentiality of the user's password.

3. Start conducting security entrance and exit briefings, and start implementing a security training program.

4. Establish criteria to determine who is allowed access to the computer room.

5. Establish a contingency plan for alternate site processing.

Management Comments

We provided a draft of this report to the Director, Defense Commissary Agency, on September 17, 1992, for comments. On October 14, 1992, we received comments from the Director, Defense Commissary Agency. The complete text of the Director's comments on all recommendations is in Enclosure 1.

The Director, Defense Commissary Agency, nonconcurred with Recommendation 1. and concurred with Recommendations 2. through 5. Overall, he stated that the Defense Commissary Agency recognized the need for automated information system security measures and that a detailed action plan to formalize the DeCA Automated Information Systems Security Program had been developed. He also stated that a number of measures have been implemented in the East Service Center that satisfy minimum security in a cost-effective manner. He also provided the following specific comments on recommendations in the draft quick-reaction audit report.

Recommendation 1. The Director stated that "DeCA's commercial off-the-shelf (COTS) hardware/software systems are not designed to implement this recommendation." However, the Director added that his agency can initiate action to bond or certify system administrators at a level consistent with the global access requirements of their positions.

Recommendation 2. The Director stated that since June 10, 1992, all users have been operating under unique logins and passwords randomly generated by a computer process. He also stated that, effective November 1, 1992, the primary responsibility for system security and password administration would reside with a recently recruited system analyst. The system analyst, rather than the systems administrator, will assume automated information system security functions.

Recommendation 3. The Director stated that beginning in June 1992, the Defense Commissary Agency initiated entrance briefing procedures for system users. He added that automated information system security awareness and training will be part of a formal DeCA Automated Information System Security Program.

Recommendation 4. The Director stated that entry into the East Service Center computer room was restricted starting in June 1992 and that a policy letter would be issued outlining the criteria and rationale for access authorizations to the computer room.

Recommendation 5. The Director stated that DeCA is in the process of purchasing disaster recovery support from a commercial source and that source will provide interim coverage until DeCA's contingency plans are developed. Commercial support is anticipated by January 1993.

Audit Response to Management Comments

Recommendation 1. Although the Director nonconcurred with the recommendation, we consider the alternative solution that he mentioned to be responsive to the recommendation. Such action would provide the Defense Commissary Agency a degree of protection that cannot be provided by the current software. We ask that the Director indicate, in response to this report, when he plans to effect the alternate solution.

Recommendation 2. Although the Director concurred with Recommendation 2., his comments were not responsive. In describing DeCA's corrective actions, he stressed that a computer generated the passwords. This is more secure than allowing individuals to generate passwords; however, the passwords that the computer generated were still being distributed, as of October 28, 1992, to users by the system administrator. The system administrator also maintained listings showing passwords that the computer generated. As stated in our discussion, we believe that it is inappropriate and unnecessary for anyone to have another user's password, because the concept of password protection is undermined. We ask the Director to reconsider his position on this recommendation.

Recommendations 3., 4., and 5. The management comments were responsive and actions taken satisfy the intent of these Recommendations. However, the Director's comments did not provide the estimated dates of implementing the formal DeCA Automated Information System Security Program and for issuing the policy letters described in Recommendations 3. and 4., respectively. We ask that the Director provide these dates in response to this report.

DoD Directive 7650.3 requires that audit recommendations be resolved promptly. Therefore, the Director, Defense Commissary Agency, must provide final comments on the unresolved recommendations by December 30, 1992. As required by DoD Directive 7650.3, the comments must indicate concurrence or nonconcurrence in the finding and each recommendation addressed to you. If you concur, describe the corrective actions taken or planned, the completion dates for actions already taken, and the estimated dates for completion of planned actions. If you nonconcur, state your specific reasons for each nonconcurrence. If appropriate, you may propose alternative methods for accomplishing desired improvements. Recommendations are subject to mediation, in accordance with DoD Directive 7650.3, in the event of nonconcurrence or failure to comment.

The courtesies extended to the audit staff are appreciated. If you have questions regarding this report or need additional information, please contact Mr. Rayburn H. Stricklin, Program Director, at (703) 614-3965 (DSN 224-3965) or Mr. Robert L. Shaffer, Project Manager, at (703) 614-1416 (DSN 224-1416). Activities visited or contacted during the audit are listed in Enclosure 2. Copies of this report are being distributed to the activities listed in Enclosure 3.

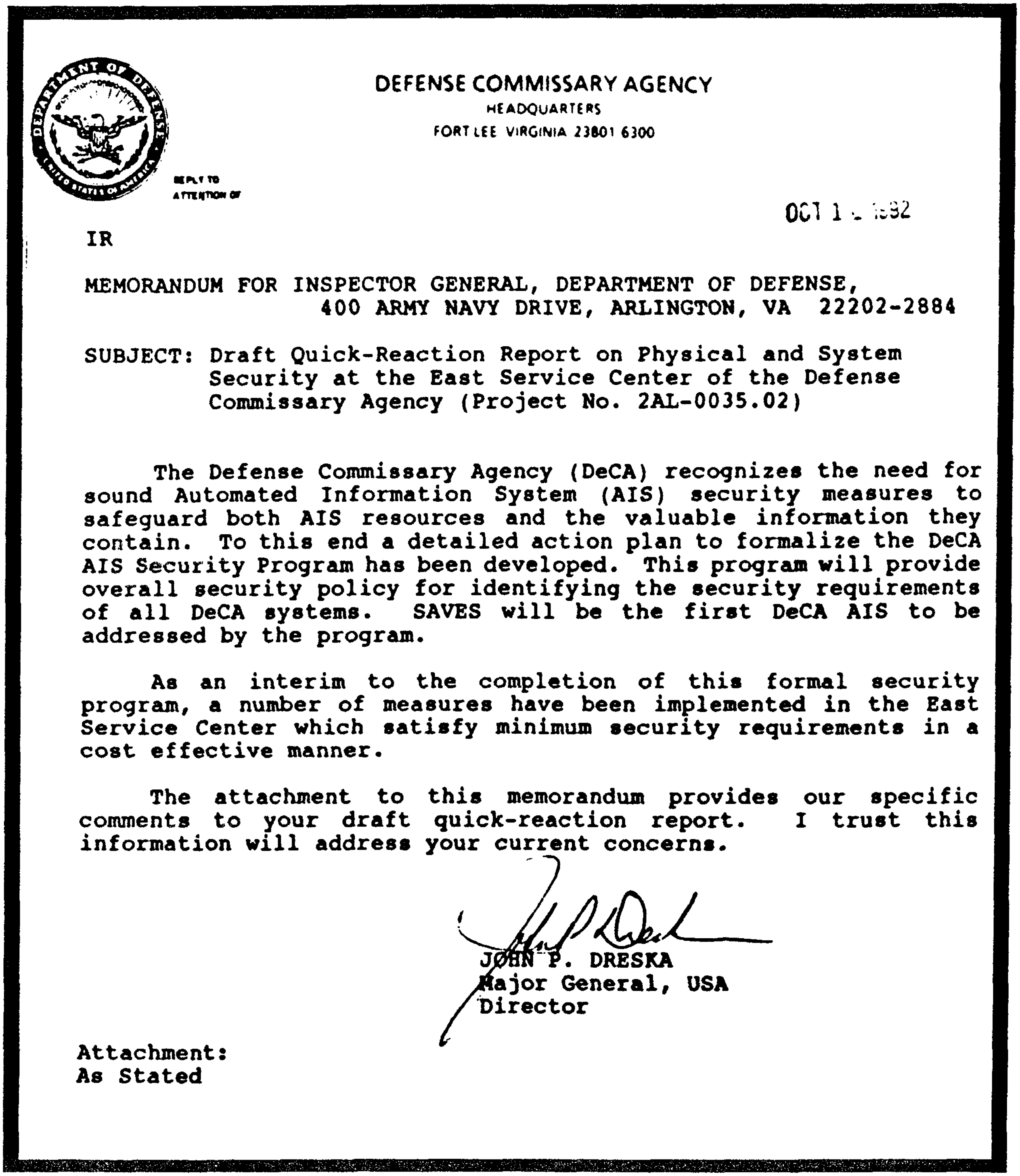
Robert J Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Enclosures

cc:
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Assistant Secretary of Defense (Production and Logistics)

Defense Commissary Agency Comments



DEFENSE COMMISSARY AGENCY
HEADQUARTERS
FORT LEE VIRGINIA 23801 6300

REPLY TO
ATTENTION OF

OCT 1 [illegible] 1992

IR

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE,
400 ARMY NAVY DRIVE, ARLINGTON, VA 22202-2884

SUBJECT: Draft Quick-Reaction Report on Physical and System Security at the East Service Center of the Defense Commissary Agency (Project No. 2AL-0035.02)

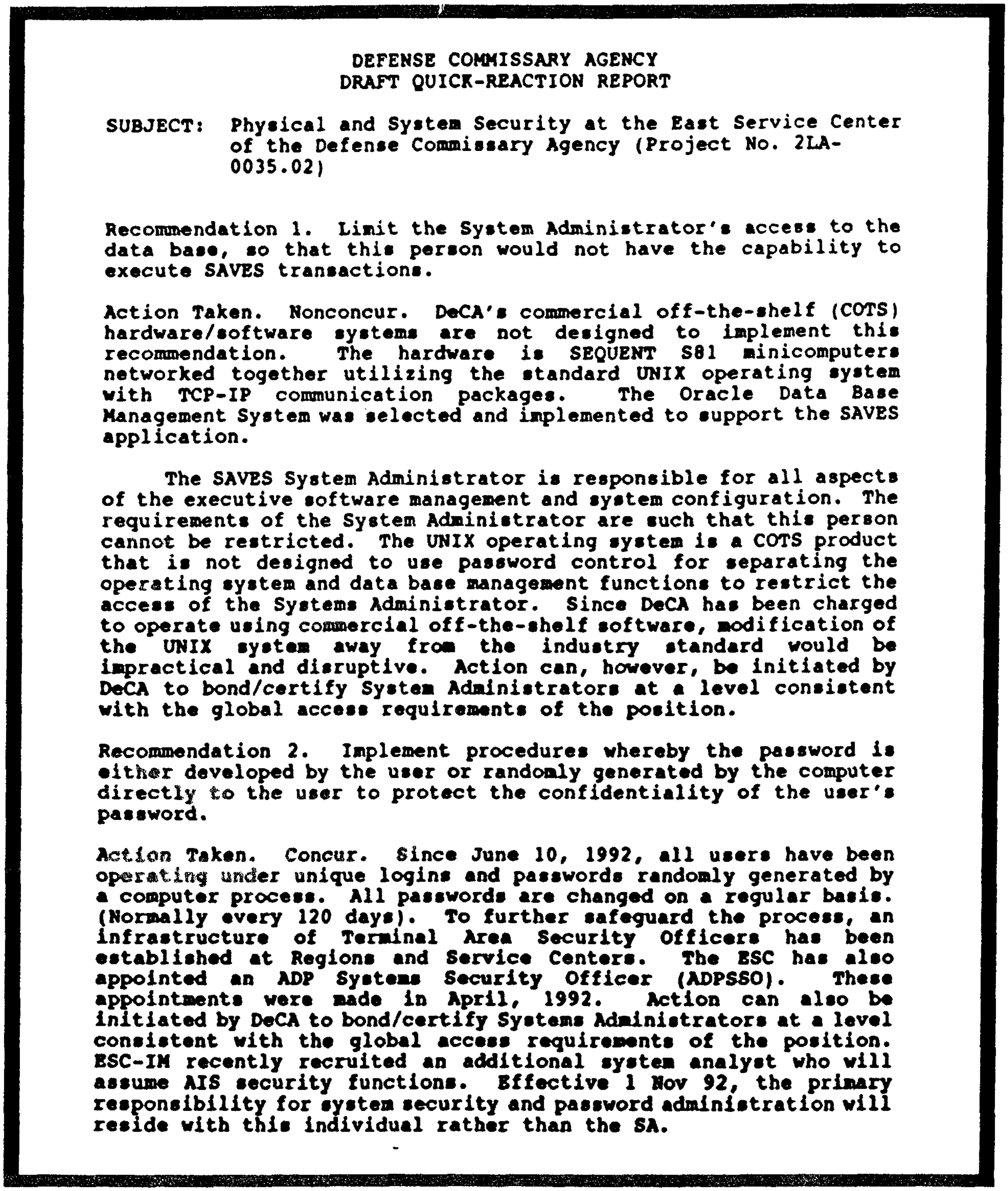
The Defense Commissary Agency (DeCA) recognizes the need for sound Automated Information System (AIS) security measures to safeguard both AIS resources and the valuable information they contain. To this end a detailed action plan to formalize the DeCA AIS Security Program has been developed. This program will provide overall security policy for identifying the security requirements of all DeCA systems. SAVES will be the first DeCA AIS to be addressed by the program.

As an interim to the completion of this formal security program, a number of measures have been implemented in the East Service Center which satisfy minimum security requirements in a cost effective manner.

The attachment to this memorandum provides our specific comments to your draft quick-reaction report. I trust this information will address your current concerns.

JOHN P. DRESKA
Major General, USA
Director

Attachment:
As Stated



DEFENSE COMMISSARY AGENCY
DRAFT QUICK-REACTION REPORT

SUBJECT: Physical and System Security at the East Service Center of the Defense Commissary Agency (Project No. 2LA-0035.02)

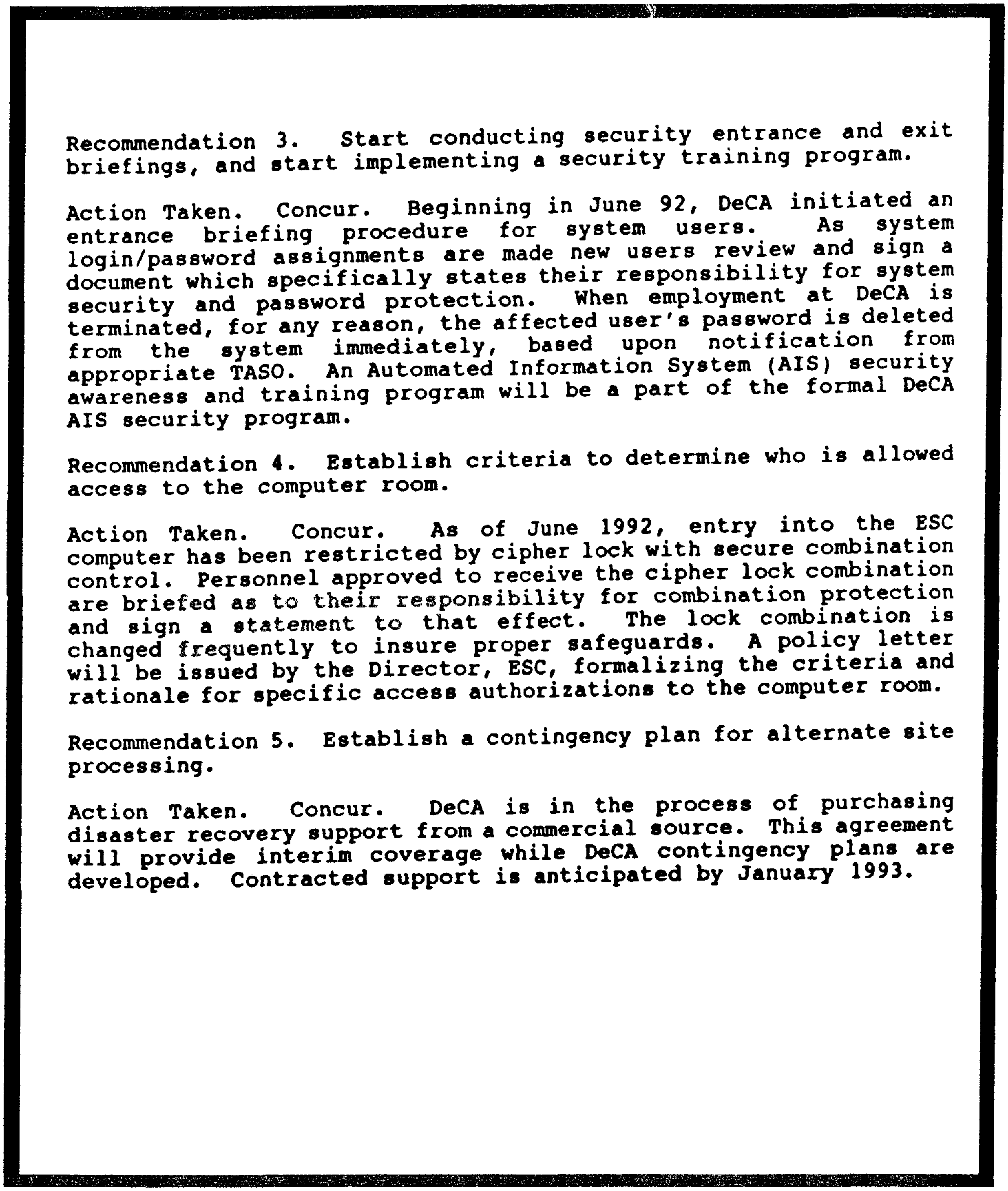
Recommendation 1. Limit the System Administrator's access to the data base, so that this person would not have the capability to execute SAVES transactions.

Action Taken. Nonconcur. DeCA's commercial off-the-shelf (COTS) hardware/software systems are not designed to implement this recommendation. The hardware is SEQUENT S81 minicomputers networked together utilizing the standard UNIX operating system with TCP-IP communication packages. The Oracle Data Base Management System was selected and implemented to support the SAVES application.

The SAVES System Administrator is responsible for all aspects of the executive software management and system configuration. The requirements of the System Administrator are such that this person cannot be restricted. The UNIX operating system is a COTS product that is not designed to use password control for separating the operating system and data base management functions to restrict the access of the Systems Administrator. Since DeCA has been charged to operate using commercial off-the-shelf software, modification of the UNIX system away from the industry standard would be impractical and disruptive. Action can, however, be initiated by DeCA to bond/certify System Administrators at a level consistent with the global access requirements of the position.

Recommendation 2. Implement procedures whereby the password is either developed by the user or randomly generated by the computer directly to the user to protect the confidentiality of the user's password.

Action Taken. Concur. Since June 10, 1992, all users have been operating under unique logins and passwords randomly generated by a computer process. All passwords are changed on a regular basis. (Normally every 120 days). To further safeguard the process, an infrastructure of Terminal Area Security Officers has been established at Regions and Service Centers. The ESC has also appointed an ADP Systems Security Officer (ADPSSO). These appointments were made in April, 1992. Action can also be initiated by DeCA to bond/certify Systems Administrators at a level consistent with the global access requirements of the position. ESC-IM recently recruited an additional system analyst who will assume AIS security functions. Effective 1 Nov 92, the primary responsibility for system security and password administration will reside with this individual rather than the SA.



Recommendation 3. Start conducting security entrance and exit briefings, and start implementing a security training program.

Action Taken. Concur. Beginning in June 92, DeCA initiated an entrance briefing procedure for system users. As system login/password assignments are made new users review and sign a document which specifically states their responsibility for system security and password protection. When employment at DeCA is terminated, for any reason, the affected user's password is deleted from the system immediately, based upon notification from appropriate TASO. An Automated Information System (AIS) security awareness and training program will be a part of the formal DeCA AIS security program.

Recommendation 4. Establish criteria to determine who is allowed access to the computer room.

Action Taken. Concur. As of June 1992, entry into the ESC computer has been restricted by cipher lock with secure combination control. Personnel approved to receive the cipher lock combination are briefed as to their responsibility for combination protection and sign a statement to that effect. The lock combination is changed frequently to insure proper safeguards. A policy letter will be issued by the Director, ESC, formalizing the criteria and rationale for specific access authorizations to the computer room.

Recommendation 5. Establish a contingency plan for alternate site processing.

Action Taken. Concur. DeCA is in the process of purchasing disaster recovery support from a commercial source. This agreement will provide interim coverage while DeCA contingency plans are developed. Contracted support is anticipated by January 1993.

ACTIVITIES VISITED OR CONTACTED

Office of the Secretary of Defense

Assistant Secretary of Defense (Production and Logistics),
  Washington, DC
Deputy Assistant Secretary of Defense (Information Systems),
  Washington, DC

Defense Agency

Defense Commissary Agency
  Headquarters, Fort Lee, VA
  East Service Center, Fort Lee, VA
  West Service Center, Kelly AFB, TX

REPORT DISTRIBUTION

Office of the Secretary of Defense

Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
Assistant Secretary of Defense (Production and Logistics)
Comptroller of the Department of Defense
Deputy Assistant Secretary of Defense (Information Systems)

Defense Agencies

Director, Defense Commissary Agency
Director, Defense Information Systems Agency

Non-DoD Activities

Office of Management and Budget
U.S. General Accounting Office, National Security and International Affairs Division, Technical Information Center

Chairman and Ranking Minority Member of the Following Congressional Committees and Subcommittees:

Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Legislation and National Security, Committee on Government Operations

AUDIT TEAM MEMBERS

Donald E. Reed, Director, Acquisition Management Directorate
Thomas F. Gimble, Deputy Director
Rayburn H. Stricklin, Program Director
Robert L. Shaffer, Project Manager
Delesta McGlone, Team Leader
George A. Leighton, Team Leader
Andrew Forte, Auditor
Robert Sacks, Auditor
John Huddleston, Auditor